Remarks

The following is in response to the Office Action dated October 31, 2003.

Per the above amendment, the abstract and pages 3 and 13 of the specification have been amended to obviate the objections noted in the Office Action. Without limitation, the support for the amendment to page 3 is provided on page 9, lines 10-11.

Further per the above amendment, claims 1-6 have been canceled, and new claims 7-28 added.

It is respectfully submitted that claims 7-28 are patentable over the prior art cited by the examiner per the following.

In Bennett et al (U. S. Patent No. 4,864,615), the apparatus of Fig. 1A corresponds to a contents-information encrypting apparatus while the apparatus of Fig. 1B corresponds to a contents-information decrypting apparatus.

Encrypting Methods and Apparatuses of the Present Invention

It was assumed in the Office Action that the first-key generation data 17 in Fig. 1A in Bennett et al corresponds to the first-key base information in the present invention. In Bennett et al, a first key 20 is generated in response to the first-key generation data 17 and also in response to a first-key prekey 18. First key 20 is used to generate a scrambled information signal 27. Therefore, in this case, Bennett et al disclose generating a first-key signal representative of a first key from first-key base information, and encrypting contents information into encryption-resultant contents information in response to the first-key signal in the present invention.

An inventive feature of the present invention is that a second-key signal representative of a second key is generated from second-key base information, and at least a portion of the first-key base information is encrypted in response to the second-key signal to convert the first-key base information into encryption-resultant first-key base information.

Assume that the first-key prekey 18 in Bennett et al corresponds to the second-key base information in the present invention. In Bennett et al, another key different from the first key 20 is not generated from the first-key prekey 18 (the second-key base information in the present invention), and the first-key generation data 17 which corresponds to the first-key base information in the present invention is not encrypted in response to another key generated from the first-key prekey 18. Therefore, in this scenario, Bennett et al do not teach the above-indicated feature of the present invention that a second-key signal representative of a second key is generated from second-key base information, and at least a portion of the first-key base information is encrypted in response to the second-key signal to convert the first-key base information into encryption-resultant first-key base information.

Assume that a second key 22 in Bennett et al corresponds to the second-key base information in the present invention. In Bennett et al, another key different from the first key 20 is not generated from the second key 22 (the second-key base information in the present invention), and the first-key generation data 17 which correspond to the first-key base information in the present invention is not encrypted in response to another key generated from the second key 22. Therefore, also in this scenario, Bennett et al do not teach the above-indicated feature of the present invention that a second-key signal representative of a second key is generated from second-key base information, and at least a portion of the first-key base information is encrypted in response to the second-key signal to convert the first-key base information into encryption-resultant first-key base information.

Assume that the first-key prekey 18 in Fig. 1A in Bennett et al corresponds to the first-key base information in the present invention. In Bennett et al, the first key 20 is generated in response to the first-key generation data 17 and also in response to the first-key prekey 18, and the first key 20 is used to generate a scrambled information signal 27. Therefore, also in this scenario, Bennett et al do not disclose generating a first-key signal representative of a first key from first-key base information, and encrypting contents information into encryption-resultant contents information in response to the first-key signal in the present invention.

As previously mentioned, an inventive feature of the present invention is that a second-key signal representative of a second key is generated from second-key base information, and at least a portion of the first-key base information is encrypted in response to the second-key signal to convert the first-key base information into encryption-resultant first-key base information.

Now assume that the first-key generation data 17 in Bennett et al corresponds to the second-key base information in the present invention. In Bennett et al, another key different from the first key 20 is not generated from the first-key generation data 17 (the second-key base information in the present invention), and the first-key prekey 18 which corresponds to the first-key base information in the present invention is not encrypted in response to another key generated from the first-key generation data 17. Therefore, also in this scenario, Bennett et al do not teach the above-indicated feature of the present invention that a second-key signal representative of a second key is generated from second-key base information, and at least a portion of the first-key base information is encrypted in response to the second-key signal to convert the first-key base information into encryption-resultant first-key base information.

Assume that the second key 22 in Bennett et al corresponds to the second-key base information in the present invention. In Bennett et al, another key different from the first key 20 is not generated from the second key 22 (the second-key base information in the

present invention), and the first-key prekey 18 which corresponds to the first-key base information in the present invention is not encrypted in response to another key generated from the second key 22. Therefore, also in this scenario, Bennett et al do not teach the above-indicated feature of the present invention that a second-key signal representative of a second key is generated from second-key base information, and at least a portion of the first-key base information is encrypted in response to the second-key signal to convert the first-key base information into encryption-resultant first-key base information.

Thus, in the cases where either the first-key generation data 17 or the first-key prekey 18 in Bennett et al is assumed to be the first-key base information in the present invention, the encrypting methods and apparatuses of the present invention nonetheless are different from the apparatus of Fig. 1A in Bennett et al.

Furthermore, Bennett et al fail to teach the authentication value in the present invention.

Widmer (U. S. Patent No. 4,313,031) does not teach the above-indicated feature of the present invention.

Accordingly, claims directed to the encrypting methods and apparatuses are patentable over Bennett et al and Widmer.

Decrypting Methods and Apparatuses of the Present Invention

The feature of the prevent invention is that an authentication value is generated from a decryption-side ID information peculiar to a decryption side and previously-fed issue ID information which has been generated by an encryption-resultant contents information provider side, and the generated authentication value is equal to an authentication value used to generate the transmission-purpose key base information.

Bennett et al fail to teach the authentication value in the present invention. Furthermore, Bennett et al do not teach the above-indicated feature of the present invention.

Widmer does not teach the above-indicated feature of the present invention.

Accordingly, it is respectfully submitted that claims directed to the decrypting methods and apparatuses are patentable over Bennett et al and Widmer.

In view of the foregoing, all of the claims pending in this application are believed to be patentable over the prior art. Accordingly, the examiner is respectfully requested to reconsider the application and pass the case to issue at an early date.

Respectfully submitted,

Louis Woo, Reg. No. 31,730
Law Offices of Louis Woo
717 North Fayette Street
Alexandria, Virginia 22314
Phone: (703) 299-4090

Date: Jan 16 2004